PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 5 : H03M 13/00

A1

(11) International Publication Number: WO 93/06662

(43) International Publication Date: 1 April 1993 (01.04.93)

(21) International Application Number: PCT/NO92/00156

(22) International Filing Date: 21 September 1992 (21.09.92)

(30) Priority data:
913705 20 September 1991 (20.09.91) NO

(71) Applicants (*for all designated States except US*): ABB SIGNAL AB [SE/SE]; P.O. Box 42505, S-126 12 Stockholm (SE). ABB TEKNOLOGI AS [NO/NO]; P.O. Box 90, N-1361 Billingstadsletta (NO).

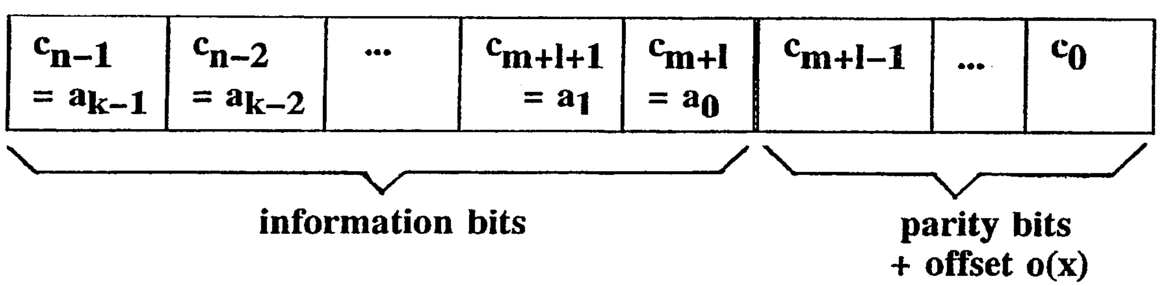
(72) Inventors; and
(75) Inventors/Applicants (*for US only*) : ENDRESEN, Jan [NO/NO]; Borgenveien 146, N-1362 Billingstad (NO). CARLSON, Erik [NO/NO]; Karl Pedersens vei 45, N-1456 Nesoddhøgda (NO).

(74) Agent: A/S OSLO PATENTKONTOR DR. ING. K.O. BERG; P.O. Box 7007 H, N-0306 Oslo (NO).

(81) Designated States: FI, NO, US, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, SE).

Published
With international search report.

(54) Title: METHOD FOR CODING AND DECODING A DIGITAL MESSAGE



(57) Abstract

The present invention relates to a method for coding and transmitting a digital message (c(x)) comprising a first number of information bits (a(x)) and a second number of control bits (b(x)), said message or code word being normally transmitted continuously, as well as a method for receiving and decoding such a digital message. In order to allow for a reliable block synchronization and error detection, there is according to the invention suggested a code format by which there is avoided the need to wait for a start of a block or message, and by which there is allowed verification before synchronisation.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	FI	Finland	MN	Mongolia
AU	Australia	FR	France	MR	Mauritania
BB	Barbados	GA	Gabon	MW	Malawi
BE	Belgium	GB	United Kingdom	NL	Netherlands
BF	Burkina Faso	GN	Guinea	NO	Norway
BG	Bulgaria	GR	Greece	NZ	New Zealand
BJ	Benin	HU	Hungary	PL	Poland
BR	Brazil	IE	Ireland	PT	Portugal
CA	Canada	IT	Italy	RO	Romania
CF	Central African Republic	JP	Japan	RU	Russian Federation
CG	Congo	KP	Democratic People's Republic of Korea	SD	Sudan
CH	Switzerland			SE	Sweden
CI	Côte d'Ivoire	KR	Republic of Korea	SK	Slovak Republic
CM	Cameroon	LI	Liechtenstein	SN	Senegal
CS	Czechoslovakia	LK	Sri Lanka	SU	Soviet Union
CZ	Czech Republic	LU	Luxembourg	TD	Chad
DE	Germany	MC	Monaco	TG	Togo
DK	Denmark	MG	Madagascar	UA	Ukraine
ES	Spain	ML	Mali	US	United States of America

Method for coding and decoding a digital message.

Field of the invention

The present invention relates to a method for coding and transmitting a digital message comprising a first number of information bits and second a number of control bits, said message or code word being normally transmitted continuously.

Further, the invention relates to a method for receiving and decoding a transmitted digital message comprising a first number of information bits and a second number of control bits, said message or code word being received normally continuously.

Background of the invention

The present invention has been developed in connection with automatic train control systems, but should not be limited to such systems. Further, the present invention has been developed in connection with intermittent communication, in which the communication can last only for a certain period of time due to physical constraints, but neither shall the invention be limited to this specific type of communication.

However, in the present specification the invention will be explained in connection with for example an automatic train system.

Prior art

In intermittent communication which due to physical constraints can only last for a certain period, it is important to maximize the information transferred for a given reliability. An example is a train passing a radio beacon which transmits a message containing control

information. The normal way to solve this problem is for the beacon to transmit a known synchronization bit pattern before the message. This may put a constraint on the information in the message to avoid false synchronization. To ensure that the train receives at least one complete message, it is necessary to allow time for almost two messages to be received since the receiver could just miss the first bit of a message and therefore have to wait for the next message.

Another way of solving the synchronization problem is to slave the radio beacon to the train receiver, but this is more complex and requires a transmitter in the train. The message is repeatedly transmitted by the beacon to increase the probability of correct reception. Those aspects of the system that are relevant can be summarized as follows.

* The beacon transmits a binary message of the given length n. This message is repeated without gaps for as long as the beacon gets enough power.

* The receiver must be able to determine the block boundaries in the received data stream.

* The probability of undetected error (the reliability) of the transmission must be guaranteed.

<u>Objects of the present invention</u>

An object of the present invention is to provide a method, in which there is avoided the need to wait for a start of a block or message, and in which there is allowed data verification before synchronization.

Another object of the present invention is to provide a method, in which the received telegram can be as short as the length of the message or code word.

Yet another object of the present invention is to provide a method, in which the receiving time can be reduced to a minimum.

Still another object of the present invention is to provide a method, in which the probability of receiving a correct message and the correct synchronization thereof is guaranteed.

Further, an object of the present invention is to use error control codes in a new way giving a new code format in which error control and synchronization are combined in the same parity bits.

Disclosure of the invention

In connection with a method as stated in the introductory part, the above objects are achieved in that on the transmitter side there is selected a generator polynomial producing a cyclic code, that said information bits are divided by said generator polynomial for thereby generating a remainder polynomial which is included in the message to be transmitted as said second number of control bits.

Thereby is achieved a valid code word provided the correct number of bits are received, but independent of the synchronization shift or start bit thereof.

In order to facilitate the control of any synchronization shift in the message or code word it is required that on the transmitter side there are selected first and second polynomials both being generators for cyclic codes, which polynomials are multiplied with each other, and that said information bits are divided by said products for thereby generating a remainder polynomial which is included in the message to be transmitted as said second number of control bits, and more specifically in that the first of the two cyclic code generator polynomials is used for controlling

error detecting capability of the message in question, whereas the second of the two cyclic code generator polynomials is used for acquiring synchronization.

In a specific embodiment the length of the digital message or code word comprises a specific number of n bits, and there is used first and second selected generator polynomials which both produce cyclic code words of length n, said second generator polynomial being irreducible and not a factor in said first generator polynomial.

In a still more specific embodiment an offset polynomial is added modulo 2 to the remainder of the code word in question, the offset polynomial being divisable by the error control generator polynomial but not the synchronization generator polynomials.

Consequently, at the receiver side the method according to the present invention is characterized in that the message or code word is registered as such independently of the sequential appearance of the start of the information bits as long as the correct number of bits (n) in one message block are received.

Further features and advantages relating to the present invention will appear from the following detailed description, reference being made to the appending drawings.

Brief disclosue of the drawings

Fig. 1 illustrates the format of a code word block.

Fig. 2 illustrates the polynomial corresponding to the data seen through a window of length n.

Detailed description of embodiments

The present invention will now be explained in general terms,

The present invention will now be explaned in general terms, it being understood that the invention suggests using error control codes in a new way, for thereby generating a new code format in which error control and synchronization are combined in the same parity bits.

The code format

Binary vectors will be denoted by polynomials, e.g. the vector $v = [v_{k-1},...,v_1,v_0]$, is represented by the polynomial $v(x) = v_{k-1}x^{k-1}..+ v_1x + v_0$. For references on coding theory see ref.1, 2 and 3.

The transmitted message (the code word) will be denoted by $c = [c_{n-1} ...c_1,c_0]$, corresponding to the polynomial $c(x)$. The order of transmission is from left to right, i.e.c_{n-1} is the bit transmitted first, then c_{n-2}, etc, and c_0 is transmitted last. The same message is repeated continually.

The transmitted messages are code words in a cyclic code of length n, the generator polynomial of which will be called $g(x)$; i.e. $c(x)$ is divisible by $g(x)$. A cyclic code is such that every valid code word can be divided into two parts and the parts interchanged, and the new code word will still be valid. The error detecting and error correcting capability of the proposed scheme comes from $g(x)$. The degree of $g(x)$ will be denoted by m.

A second polynomial, which will be denoted by $f(x)$, will be used for synchronization. The polynomial $f(x)$

* is irreducible
* divides $x^n- 1$ but does not divide x^m-1 for $0<m<n$,
* is not a factor of $g(x)$.

These constraints are easily satisfied and still leave some freedom in the choice of $f(x)$. The degree of $f(x)$ will be

denoted by 1. The above constraints ensure that any cyclic shift of the code word has a unique syndrome with respect to f(x).

For any two polynomials h(x) and p(x) non zero, let $R_{p(x)}[h(x)]$ denote the unique polynomial r(x) of degree less than deg[p(x)] that satisfies h(x)= q(x)p(x) + r(x), i.e, it is the remainder that results from dividing h(x) by p(x).

Let a(x) be the information polynomial, i.e, the polynomial corresponding to the binary vector $[a_{k-1}, \ldots a_1, a_0]$ of information bits. The number k of information bits equals n-1-m. Note that there is no constraint on the information bits,i.e, all 2^k possibilities are allowed.

The encoding rule is:

$$c(x) = x^{m+1}\,a(x)+R_{f(x)g(x)}\,[x^{m+1}a(x)]+o(x).$$

The multiplication of a(x) with the factor x^{m+1} has the effect of shifting the information m+1 to the left, leaving m+1 bits free for the parity and offset bits.

The remainder is calculated with respect to the product of f(x) and g(x). The binary polynomial o(x) ("offset") is used for synchronization. It is divisable by g(x) but not f(x), and its degree is smaller that m + 1. Any binary polynomial satisfying these constraints can be used; and as for f(x) above, there is no reason to choose a particular o(x). The resulting code format is shown in Fig.1.

The bits are transmitted from left to right,i.e, in the order $c_{n-1}, c_{n-2}, \ldots, c_1, c_0, c_{n-1}, c_{n-2} \ldots$

Since o(x) is divisible by g(x), c(x) is always divisible by g(x) and is therefore a code word in the cyclic code generated by g(x). Note also that c(x)-o(x) is divisible by f(x), but c(x) is not.

The central idea of this code format is that in the absence of errors, any block of length n that is cut out of the transmitted data stream is a code word in the cyclic code generated by g(x). Any such block is thus protected by the full error-detecting capability provided by g(x). The code format of this section may be used with a varity of codes.

<u>Decoding</u>

The basic operation to be performed by the receiver is thus as follows:

1. Receive a block of n bits.

2. Look at a given window of length n. Verify this code word with respect to g(x). If this is possible, go to step 3; otherwise shift the window and do step 2 again.

3. Recover data from window based on parity check with respect to f(x).

As an alternative, the shifting of the windows in the case of an unsuccessful decoding attempt can be left out. Permitting this shifting of the window increases the probability of successful transmission but also the probability of undetected error.

Now, consider point 3 of this procedure, i.e. the recovery of the information from the window. Let w(x) be the polynomial that corresponds to the data block as seen through a window of length n that is shifted by s positions with respect to the block boundaries of the transmitted data, see Fig.2.

If s is the shift between the block boundaries of the data stream and the window, then $w(x)=R_{x^n-1}[x^s \cdot c(x)]$, provided

In the absence of errors, $w(x) = R_{x^{n}-1}[x^{s}c(x)]$. The result of the computation

$$
\begin{aligned}
R_{f(x)}[w(x)] &= R_{f(x)}[R_{x^{n}-1}[x^{s}c(x)]] \\
&= R_{f(x)}[x^{s}c(x)] \\
&= R_{f(x)}[x^{s}R_{f(x)}[c(x)]] \\
&= R_{f(x)}[x^{s}o(x)]
\end{aligned}
$$

shows that all shift s in the range 0.....n-1 have unique syndrome $R_{f(x)}[w(x)]$. For, let s and s', s≤s' be two shifts in that range, and consider $R_{f(x)}[x^{s}o(x)]-R_{f(x)}[x^{s'}o(x)] = R_{f(x)}[x^{s}(1-x^{s'-s})o(x)]$. Since both x_s and o(x) have no common factors with f(x), this expression is zero if and only if f(x) divides $1-x^{s'-s}$; but since n is the smallest interger such that f(x) divides $x^{n}-1$, this implies s' = s. The information a(x) can thus easily be recovered from w(x): i.e. shifting w(x) cyclically s times to the right yields c(x).

References

1. W.W.Peterson and E.J.Weldon, Jr. Error-Correcting Codes, 2nd edition, Cambridge : MIT Press, 1972.

2. R.E.Blahut, Theory and Practice of Error Control Codes, Addison-Wesley, 1983.

3. Shu Lin and D.J. Costello, Error Control Coding, Fundamentals and Applications, Prentice Hall, 1983.

Patent Claims

1. Method for coding and transmitting a digital message (c(x)) comprising a first number of information bits (a(x)) and second a number of control bits (b(x)), said message or code word normally being transmitted continuously, characterized in that on the transmitter side there is selected a generator polynomial (CRC(x)) producing a cyclic code, that said information bits (a(x)) are divided by said generator polynomial (CRC(x)) for thereby generating a remainder polynomial ($c_r(x)$) which is included in the message to be transmitted as said second number of control bits (a(x),$c_r(x)$).

2. Method as claimed in claim 1, characterized in that on the transmitter side there are selected first and second polynomials (g(x) and f(x)) both being generators for cyclic codes, which polynomials are multiplied with each other, and that said information bits (a(x) are divided by said product (g(x)*f(x)) for thereby generating a remainder polynomial ($c_r(x)$) which is included in the message to be transmitted as said second number of control bits (a(x),$c_r(x)$).

3. Method as claimed in claim 1 or 2, characterized in that a first of the two cyclic code generator polynomials (g(x)) is used for monitoring error detecting capability of the message in question, whereas a second of the two cyclic code generator polynomials (f(x)) is used for acquiring synchronization.

4. Method as claimed in claim 2 or 3, characterized in that the length of the digital message or code word (c(x)) comprises a specific number of n bits (for example 255), and that there are used first and second selected generator polynomials (g(x) and f(x) which both produce cyclic code words of length n, and that one generator polynomial (f(x)) is irreducible and not

a factor in the other generator polynomial (g(x)).

5. Method as claimed in claim 3 or 4, c h a r a c t e r i z e d i n that an offset polynomial (o(x)) is added modulo 2 to the remainder of the code word in question, and that the offset polynomial (o(x)) is divisable by the error control generator polynomial (g(x)) but not the synchronization generator polynomials (f(x)).

6. Method for receiving and decoding a transmitted digital message (c(x)) comprising a first number of information bits (a(x)) and second a number of control bits (b(x)), said message or code word being received normally continuously, c h a r a c t e r i z e d i n that at the receiver side the message or code word is registered as such independently of the sequential appearance of the start of information bits (a(x)) as long as the correct number of bits (n) in one message block are received.

7. Method as claimed in claim 6, c h a r a c t e r i z e d i n that at the receiver side the digital message or code word (c(x)) is divided by the same error control generator polynomial (g(x)) as selected on the transmitter side, whereby there is obtained a local remainder, which if zero indicates a probale error free message or code word.

8. Method as claimed in claim 6 and 7, c h a r a c t e r iz e d i n that at the receiver side the digital message or code word (c(x)) is divided by the same synchronization generator polynomial (f(x)) as selected on the transmitter side, whereby there is obtained a local remainder, which if non-zero determines uniquely the number of bits the code word has to be rotated to recover the information polynomial (a(x)).

9. Method as claimed in claim 8,

c h a r a c t e r i z e d i n that at the receiver side the digital message or code word (c(x)) is rotated and divided by the same synchronization generator polynomial (f(x)) as selected on thc transmitter side, until the local remainder is equal to the remainder obtained by dividing the offset polynomial (o(x)) by the synchronization generator polynomial (f(x)), and the information polynomial (a(x)) can be recovered from the first part of the rotated received code word (c(x)).

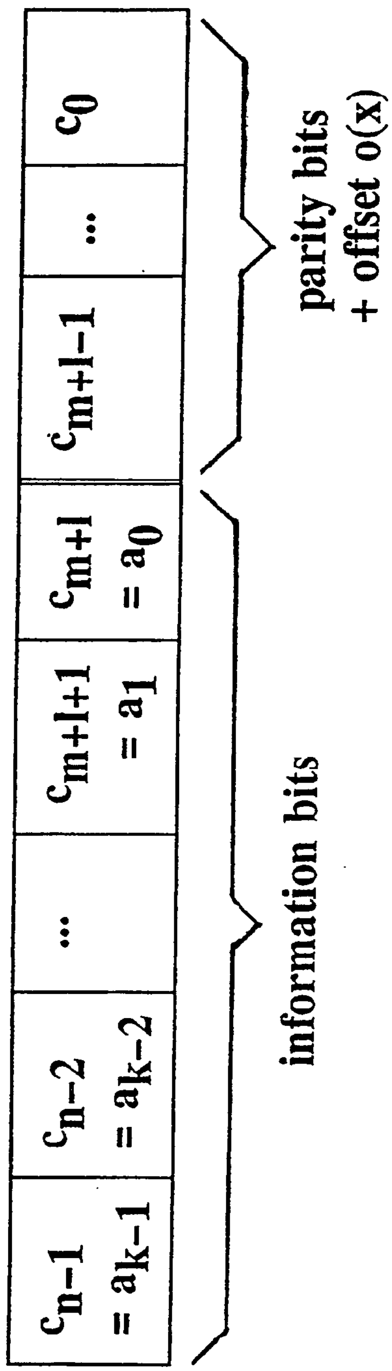
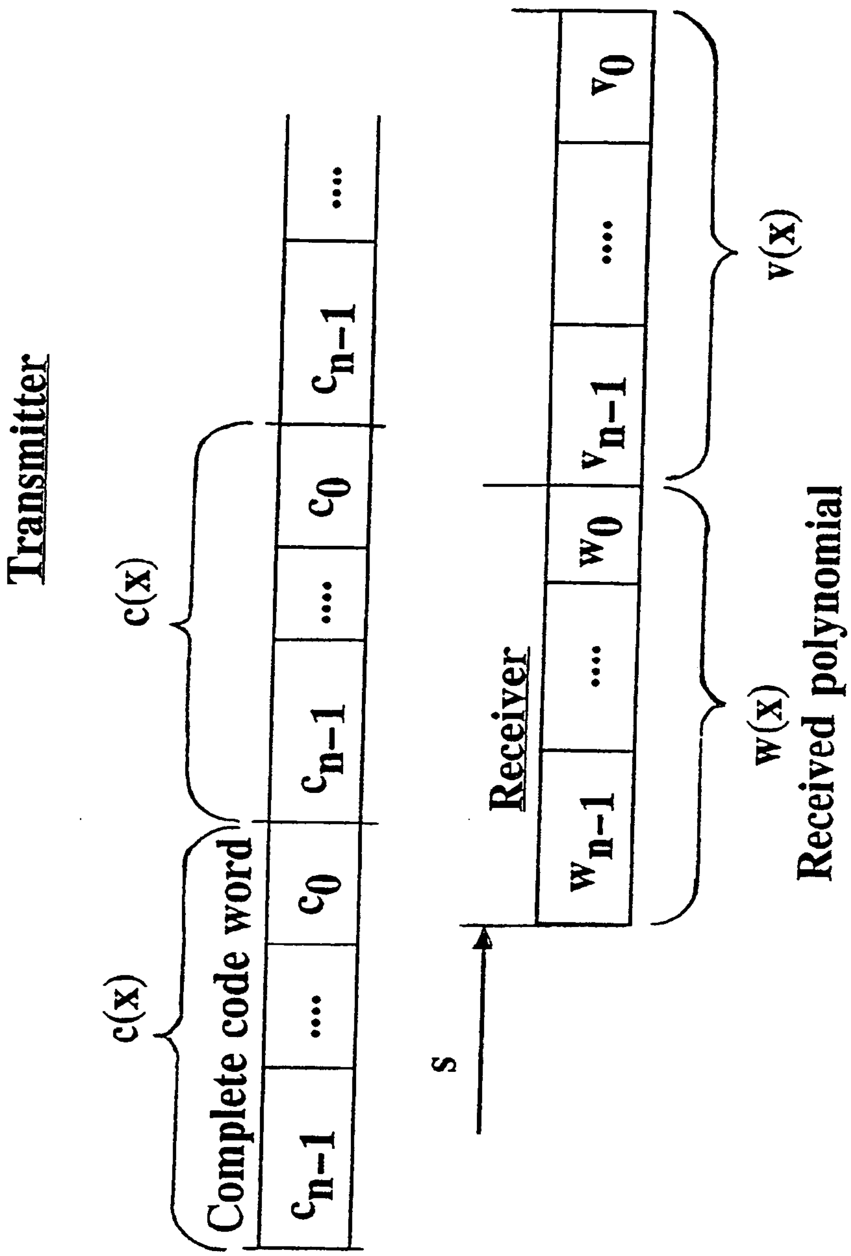

c_0
...
c_{m+l-1}
c_{m+l} $= a_0$
c_{m+l+1} $= a_1$
...
c_{n-2} $= a_{k-2}$
c_{n-1} $= a_{k-1}$
parity bits
+ offset o(x)
information bits

FIG. 1

FIG. 2


Transmitter
c(x)
Complete code word
c(x)
c_{n-1}
....
c_0
c_{n-1}
....
c_0
c_{n-1}
....
Receiver
s
w_{n-1}
....
w_0
v_{n-1}
....
v_0
w(x)
Received polynomial
v(x)

INTERNATIONAL SEARCH REPORT

International Application No PCT/NO 92/00156

I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all)[6]

According to International Patent Classification (IPC) or to both National Classification and IPC

IPC5: H03M 13/00

II. FIELDS SEARCHED

Minimum Documentation Searched[7]

Classification System	Classification Symbols
IPC5	H03M

Documentation Searched other than Minimum Documentation to the Extent that such Documents are Included in Fields Searched[8]

SE,DK,FI,NO classes as above

III. DOCUMENTS CONSIDERED TO BE RELEVANT[9]

Category *	Citation of Document,[11] with indication, where appropriate, of the relevant passages [12]	Relevant to Claim No.[13]
A	US, A, 4777635 (N. GLOVER) 11 October 1988, see the whole document --	1-9
A	WO, A1, 8500714 (TELEDIFFUSION DE FRANCE) 14 February 1985, see the whole document --	1-9
A	Chambers. Basics of communications and Coding, New York 1985; p. 122-150, "Error-correcting codes"; see the whole document --	1-9

----

* Special categories of cited documents: [10]

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance, the claimed invention cannot be considered novel or cannot be considered to involve an inventive step

"Y" document of particular relevance, the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

IV. CERTIFICATION

Date of the Actual Completion of the International Search	Date of Mailing of this International Search Report
28th December 1992	30 -12- 1992
International Searching Authority	**Signature of Authorized Officer**
SWEDISH PATENT OFFICE	Rune Bengtsson

ANNEX TO THE INTERNATIONAL SEARCH REPORT
ON INTERNATIONAL PATENT APPLICATION NO.PCT/NO 92/00156

This annex lists the patent family members relating to the patent documents cited in the above-mentioned international search report.
The members are as contained in the Swedish Patent Office EDP file on 02/12/92
The Swedish Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US-A- 4777635	88-10-11	NONE	
WO-A1- 8500714	85-02-14	CA-A- 1218461	87-02-24
		DE-A- 3475253	88-12-22
		EP-A-B- 0133137	85-02-13
		FR-A-B- 2549984	85-02-01
		JP-T- 60501930	85-11-07